

Quantum Key Distribution Using a Triggered Quantum Dot Source Emitting near 1.3 μm

P. M. Intallura,* M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, and A. J. Shields
*Toshiba Research Europe Limited, Cambridge Research Laboratory,
208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom*

P. Atkinson and D. A. Ritchie
Cavendish Laboratory, University of Cambridge, J. J. Thomson Avenue, Cambridge CB3 0HE, United Kingdom
(Dated: October 2, 2007)

We report the distribution of a cryptographic key, secure from photon number splitting attacks, over 35 km of optical fiber using single photons from an InAs quantum dot emitting $\sim 1.3 \mu\text{m}$ in a pillar microcavity. Using below GaAs-bandgap optical excitation, we demonstrate suppression of multiphoton emission to 10% of the Poissonian level without detector dark count subtraction. The source is incorporated into a phase encoded interferometric scheme implementing the BB84 protocol for key distribution over standard telecommunication optical fiber. We show a transmission distance advantage over that possible with (length-optimized) uniform intensity weak coherent pulses at 1310 nm in the same system.

PACS numbers: 03.67.Dd, 73.21.La, 78.55.cr

Keywords: quantum cryptography, quantum key distribution, qkd, single photon source, semiconductor quantum dots, pillar microcavity, III-V semiconductors, molecular beam epitaxy, optical correlation, fiber optic communication

The majority of experimental realizations demonstrating quantum key distribution (QKD) have relied on encoding information onto weak coherent pulses (WCPs).^{1,2,3} Due to the Poissonian nature of laser light, there is a finite probability of generating two or more photons per pulse from such a source. This opens up a security threat where an eavesdropper, Eve, can take advantage of these extra photons by performing a photon number splitting (PNS) attack.⁴ To compensate for this security loophole, the transmitter, Alice, has to attenuate the signal by an amount that increases with distance, which reduces the transmission rate and ultimately limits the maximum secure transmission distance to the authorized recipient, Bob.⁵ Decoy-pulse techniques have been developed to help mitigate the risks associated with multiphoton pulse emission,^{6,7} and PNS secure key distribution distances are now starting to exceed those achieved with uniform pulse intensities.⁸

A single quantum emitter will exhibit “anti-bunching” of the photon emission times,⁹ such that a regulated stream of single photons with zero probability of emitting more than one photon in any given excitation pulse can be expected. Applying an efficient single quantum emitter in a cryptographic system would outperform all other methods developed to date. Several experiments using single photons with wavelengths compatible with silicon technology have already been used for QKD. These include using a stream of single-photon pulses generated by a single nitrogen-vacancy color center in a diamond¹⁰ and emission from a quantum dot.¹¹ Telecom wavelength QKD has been achieved by using pairs of photons produced via spontaneous parametric down conversion.^{12,13}

In this letter we demonstrate QKD using an optically-excited, triggered single-photon source (SPS) emitting at

a telecom wavelength. Our source, which shows a ten-fold reduction in multi-photon emission compared to a laser, has been used to distribute keys secure from the PNS attack over 35 km along standard optical fiber. By applying a security analysis for imperfect devices (GLLP),¹⁴ we demonstrate a transmission distance advantage compared to the same system configuration incorporating uniform intensity pulses from a laser source at the same wavelength.

We have previously demonstrated that a low density of telecom wavelength dots can be achieved through a bimodal growth technique¹⁵ and we have used this method to fabricate a SPS. Our source is based on an InAs quantum dot embedded at the center of a GaAs spacer in a distributed Bragg reflector (DBR) pillar microcavity $\sim 3 \mu\text{m}$ in diameter. The DBR mirrors consist of alternating layers of GaAs and $\text{Al}_{0.98}\text{Ga}_{0.02}\text{As}$, each with a designed thickness corresponding to one-quarter optical wavelength. The cavity was formed with 11 periods on top and 30 periods on the bottom of a nominally three-optical-wavelength thick spacer layer. The sample was placed in a custom built confocal microscope which was cooled in a variable temperature continuous flow liquid helium cryostat.

Below GaAs-bandgap laser pulses at 1064 nm were used to trigger photon emission from the quantum dot. At this wavelength electron-hole pairs are created in highly excited states of the dot. The telecom wavelength quantum dots used here offer stronger confinement than dots emitting below $1 \mu\text{m}$ and several shells are expected to be confined. The photogenerated carriers are expected to thermalize down to lower energy configurations in time scales shorter than the radiative lifetime. Maximum single-photon signal from the device

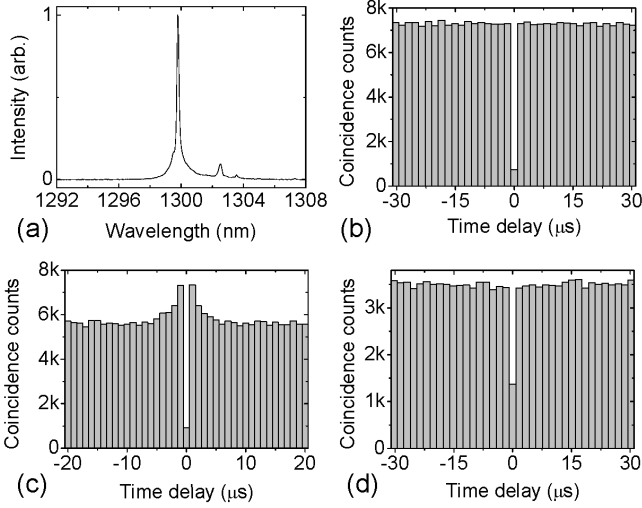


FIG. 1: a) Normalized PL spectrum recorded ~ 71 K before spectral filtering under 1064 nm excitation at saturation power. Correlation measurements (~ 71 K) on the spectrally filtered emission line with b) 1064 nm excitation pulsed at 80 MHz at low power ($\sim 102 \mu\text{W}$) with APDs gated at 594 kHz, c) 1064 nm laser excitation at 1 MHz around saturation power ($\sim 2.5 \mu\text{W}$ at this frequency) with detection at 1 MHz and d) 780 nm excitation pulsed at 80 MHz near saturation power ($\sim 57 \mu\text{W}$) with detection at 594 kHz. Counts within $150 \mu\text{s}$ of a preceding count in the same detector were rejected to limit the effect of afterpulsing. Powers quoted refer to the average power at the input of the microscope.

was achieved at ~ 71 K where a charged exciton was on resonance with the HE_{11} cavity mode [Fig. 1(a)]. We have measured suppression of $g^{(2)}(0) = 0.102 \pm 0.004$ as shown in Fig. 1(b) without any subtraction of background emission or detector dark counts. We believe that this is the lowest measured value of $g^{(2)}(0)$ reported to date from a quantum dot emitting at a telecom wavelength.

For the purpose of quantum key distribution the source was operated with excitation intensities around those where the emission line shows maximum intensity. In this case we measured $g^{(2)}(0) = 0.166 \pm 0.005$ with 1064 nm optical excitation [Fig. 1(c)]. This is markedly lower than for excitation at 780 nm where a value of $g^{(2)}(0) = 0.392 \pm 0.011$ was obtained [Fig. 1(d)]. With below-band excitation, we measure an efficiency of $\sim 5.1\%$ after coupling into single-mode fiber (SMF28). This is the highest useful efficiency reported to date at a telecom wavelength and was demonstrated with a simultaneously good $g^{(2)}(0) = 0.166$, measured without subtraction of background or detector dark counts. (The efficiency quoted above was calculated using the correlation measurement count rates. If the finite measured $g^{(2)}(0)$ is assumed to have arisen from a Poissonian background a single-photon efficiency of 4.6% would be estimated.) Even higher efficiencies may be achieved by optimizing the coupling of the source to single mode fiber and reducing the

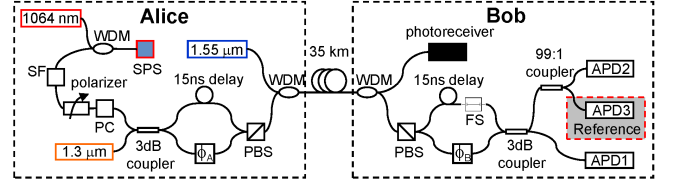


FIG. 2: A schematic diagram showing the fiber optic quantum key distribution system. SPS: single-photon source; WDM: wavelength division multiplexer; SF: spectral filter; PC: polarization controller; PBS: polarizing beam splitter/combiner; FS: fiber stretcher. Standard telecom fibers are used in the link between Alice and Bob.

roughness of the micropillars to enhance the cavity quality factor.¹⁶

Our key distribution system is based upon a time division Mach-Zender interferometer using phase modulation, as shown in Fig. 2. The system is an extension of that which our group has used to demonstrate key distribution using WCPs emitting at 1550 nm .^{17,18} However, in this case, we employ our quantum dot source in place of an attenuated laser and multiplex it with a $1.55 \mu\text{m}$ clock laser, which is used as a timing reference. The source is optically pumped with picosecond-pulsed 1064 nm laser light from a semiconductor laser diode at a frequency of 1 MHz. A third laser, emitting around the same wavelength as the source, is introduced to provide feedback to a fiber stretcher which minimizes any path mismatch in the two interfering routes.¹⁸ The BB84 protocol¹⁹ is implemented by encoding/decoding bit information through phase modulators in the two interfering paths^{1,3} and key distribution using the SPS was optimized over 35 km of optical fiber. InGaAs avalanche photodiodes (APDs) operating in gated mode at 1 MHz (~ 165 K) were used to detect the interfering single photons. The detectors used are around 9% efficient at the source wavelength and in the system each gave a typical count probability of 0.87×10^{-6} per gate with the SPS disabled. Of this we attribute a probability of 0.82×10^{-6} per gate to detector dark counts and the remainder due to stray counts originating from the lasers. We estimate a 7.9 dB loss in Alice, a 1.7 dB loss in Bob and use standard SMF28 telecom fiber with a measured loss of 12.8 dB through the fiber link. An average visibility of $\sim 99.7\%$, after dark count correction, was achieved and is shown in Fig. 3(a).

A 7 kbit sifted key was distributed with a quantum bit error rate (QBER) of 5.9% [see Fig. 3(b)]. Based on the GLLP theory for imperfect devices in Gottesman *et al.*,¹⁴ (specifically theorem 6) we can deduce that the key exchange would have been secure against the PNS attack given the measured value of $g^{(2)}(0)$ of 0.166. Eve is assumed to have the full technological capabilities necessary to access all the information carried by the residual multiphoton pulses and those pulses contributing to the QBER. In the security analysis for the SPS, the multi-

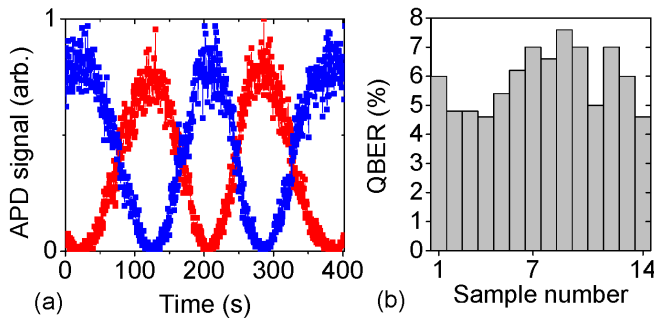


FIG. 3: a) Counts as a function of time on APD1 and APD2 showing a 98.5% visibility before dark count correction and b) variation in the QBER over the course of a key transfer over 35 km of fiber. Each bin represents a sample of 500 sifted bits.

photon probability is reduced from $\sim \mu^2/2$ in the WCP case to $\sim g^{(2)}(0) \times \mu^2/2$, where μ is the average number of photons per pulse.

We now compare the performance of our single-photon BB84 setup with that which could be achieved using 1310 nm WCPs in the same system according to GLLP theory. The comparison is made by taking the same detector gating conditions and assuming the same dark count probability and detection efficiency. In both cases the quantum bit errors in the raw key were taken to consist of half the sum of the dark and stray counts plus 2.6% of the raw bit rate due to errors in the phase modulators etc. The error correction algorithm was taken to use 1.17 times the number of bits specified in the Shannon limit.^{20,21} For each fiber length up to ~ 28 km there exists a range of μ for which unconditionally secure QKD using WCPs is possible. Between the upper bound governed by the PNS attack and a lower bound governed by the dark (and stray light) count contribution to the QBER, an optimal laser intensity exists for which the maximal secure bit rate can be obtained. It is this optimally attenuated laser performance at 1310 nm that we compare to our SPS performance in Fig. 4.

Fig. 4 shows that key distribution with our dot source has a quantitative advantage at long distances compared with that which could be securely achieved using uniform intensity laser pulses at 1310 nm. We note that for transmission distances greater than ~ 11 km a higher

bit rate is achieved with the SPS. For short transmission distances WCP systems are favorable as higher bit rates, due to the higher photon flux, can be achieved. However, this is an advantage which could be overcome by improving the performance of our SPS.

We have demonstrated single-photon quantum key distribution using a quantum dot source emitting near 1.3 μm . The source was excited below the GaAs-bandgap and showed strong suppression of multi-photon emission to $\sim 10\%$ of the Poissonian level without detector dark count subtraction. The below GaAs-bandgap excitation was responsible for the high quality single-photon emission. We distributed a key secure against the PNS attack over 35 km. These results highlight the potential advantage of single-photon QKD for long distance quantum cryptography through an existing telecom infrastructure.

The authors acknowledge partial financial support from DTI and EPSRC through LINK OSDA Programme QLED, EU through IPs SECOQC and QAP, and NoE SANDiE.

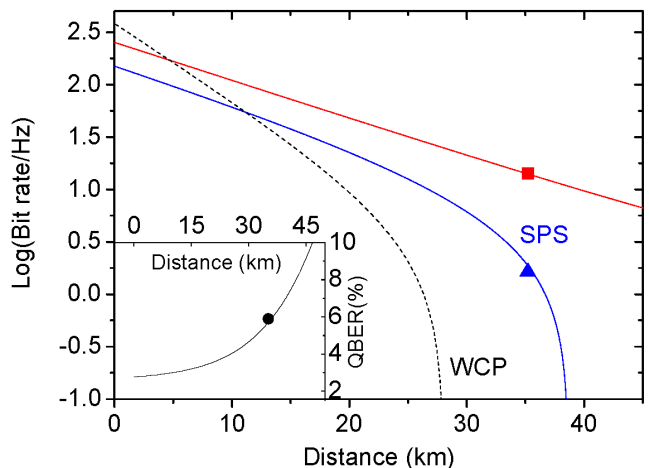


FIG. 4: Theoretical evaluation comparing the PNS secure transmission distance of our SPS (solid blue curve) with an equivalent WCP system (dashed curve). The solid red curve shows the theoretical sifted bit rate of the SPS. The data points represent our experimental sifted bit rate (square) and secure bit rate (triangle). The inset shows the calculated QBER (line) with the measured value.

* Also at Cavendish Laboratory, University of Cambridge, J. J. Thomson Avenue, Cambridge CB3 0HE, United Kingdom; Electronic address: pmi20@cam.ac.uk

¹ P. D. Townsend, J. G. Rarity, and P. R. Tapster, *Electron. Lett.* **29**, 634 (1993).

² P. D. Townsend, *Electron. Lett.* **30**, 809 (1994).

³ C. Marand, and P. D. Townsend, *Opt. Lett.* **20**, 1695 (1995).

⁴ G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders,

Phys. Rev. Lett. **85**, 1330 (2000).

⁵ C. Gobby, Z. L. Yuan, and A. J. Shields, *Electron. Lett.* **40**, 1603 (2004).

⁶ H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).

⁷ X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).

⁸ Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu, and G.-C. Guo, arXiv:0704.2941v2 [quant-ph] (2007).

⁹ H. J. Kimble, M. Dagenais, and L. Mandel, *Phys. Rev.*

- Lett. **39**, 691 (1977).
- ¹⁰ A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002).
 - ¹¹ E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vučković, G. S. Solomon, and Y. Yamamoto, Nature **420**, 762 (2002).
 - ¹² A. Trifonov, and A. Zavriyev, J. Opt. B **7**, S772 (2005).
 - ¹³ A. Soujaeff, T. Nishioka, T. Hasegawa, S. Takeuchi, T. Tsurumaru, K. Sasaki and M. Matsui, Opt. Express **15**, 726 (2007).
 - ¹⁴ D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Information and Computation **4**, 325 (2004).
 - ¹⁵ M. B. Ward, O. Z. Karimov, D. C. Unitt, Z. L. Yuan, P. See, D. G. Gevaux, A. J. Shields, P. Atkinson, and D. A. Ritchie, Appl. Phys. Lett. **86**, 201111 (2005).
 - ¹⁶ S. Reitzenstein, C. Hofmann, A. Gorbunov, M. Strauß, S. H. Kwon, C. Schneider, A. Löffler, S. Höfling, M. Kamp, and A. Forchel, Appl. Phys. Lett. **90**, 251109 (2007).
 - ¹⁷ C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
 - ¹⁸ Z. L. Yuan, and A. J. Shields, Opt. Express **13**, 660 (2005).
 - ¹⁹ C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, (IEEE, New York, 1984), p. 175.
 - ²⁰ G. Brassard, and L. Savail, Lect. Note Comput. Sci. **765**, 410 (1994).
 - ²¹ C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).